Said HASHEMI
Groupe AIS
16/05/2024

Resume

The first part:

This text talk about ethical hacking and hacking.

According to this text, I found the fact that the cyber-crimes are rising, and we hear about it all the time on the news platforms. I can cite the recent visit of President Obama and President Xi abording this subject.

This new treats in IT, persuade us to think, how we can secure our information system to protect our company's data and confidentiality. We could demand assistance from the ethical hacking services like Digital Locksmith.

To answer the question: is ethical hacking even ethical? We can add that it is a new trend in IT, we must use these methods to ensure the security of our companies.

In the hacking world, we count three groups, the black hats, grey hats, and White hats. The black hats hackers do not care about your information after hacking, they just steal information and finance their community or participants through hacking. The other group, grey hackers, are people who prove their hacking competence, but they do not aware the owner and like the first group, they do not care about the consequences of their work. The last group, white hats are ethical hackers, they test our information system issues, intrusion ways, and possible problems that could help the black hats to enter our network; they have the ability of black hats, but they are responsible for the result and need permission to start the hacking process.

Chris Kirsch, a product marketing, clarifies that the penetration tests are like doing a car crash to test the safety of the car. The penetration test is the same, it is used to test the safety and security of the network.

The second part:

Mr. John Berry,

With highest esteems,

We faced a cyber-attack recently; our team is working to ensure the normal situation and decrease the probable damages.

The issue caused by a user who did not use a VPN Tunnel to connect to our private network and tried to entre the system, but the user failed because the router which acts like a firewall too, did not authorized the access, but when the user tries to send the credentials through an application which is not equipped with VPN, an hacker succeeded to have the credentials, and used our VPN application to enter the network.

We try to secure our systems considering these issues, but we need to work with other employees to evite the next probable attacks and to increase sensibility.

We must consider the following points to prevent future attacks:

1- Using strong password.
2- Using VPN Tunnels to connect the private network.
3- Observing the prohibition of entering the session password to the websites that do not take part to our company's infrastructure.